including data that is not to be subject to tampering detection. The protected data region includes an unprotection list which lists tag names that indicate the types of data included in the unprotected data region.

For received data that is included in the protected data region, it is detected whether that data has been tampered with by using the tampering detection information included in the authentication information region. In other words, the tampering detection information from the authentication information region is used to detect whether the data that is in the protected data region has been tampered with after receipt of the data.

A determination is then made whether the data that is included in the unprotected data region is valid. This is done by determining when a tag name indicating a type of the data included in the unprotected data region coincides with the tag name in the unprotection list after it has been confirmed as not having been tampered with as discussed above.

In the telephone interview, the Examiner cited portions of Eastlake as disclosing the step of determining whether data included in the unprotected data region has been tampered with, by checking an unprotection list which lists tag names indicated types of the data included in the unprotected data region. For example, the Examiner cited the top of page 9 as discussing core validation, reference validation and signature validation. Example was made with respect to section 3.2 on page 10 of Eastlake, in which the Examiner considered section 3.2.1 to correspond, for example, to detecting whether data in an unprotected data region has been tampered with using tampering detection information from the authentication information region, and section 3.2.2 for determining whether data included in the unprotected data region has been tampered with by checking an unprotection list of tag names with the tag names in the unprotected data region.

However, in Eastlake, section 3.2.2 merely describes general signature validation methods using a public key cryptosystem. It neither discloses nor suggests providing, in a protected data region, and unprotection list including tag names indicating the type of data included in the unprotected data region. It is noted that the signature validation of section 3.2.2 involves three steps, the first canonicalizing the SignedInfo element based on the canonicalization method in the SignedInfo, the second involving obtaining keying information from KeyInfo or from an external source and the third using a specified signature method to validate the SignatureValue or the SignedInfo element. It is not seen where this supports any determination of coincidence of tag names of data included in an unprotected data region with a list of tag names indicating types of data included in an unprotection list in a protected data region. It is respectfully submitted that the Examiner's assertion that this somehow does correspond to the claimed determination is unreasonable.

As noted above, with the present invention as reflected in each of independent claims 46, 48, 50 and 51, the protected data region includes an unprotection list listing tag names indicating the types of data included in the unprotected data region. The tag contained in the unprotected data region is checked with the tag name in the unprotection list so that the validity of the data in the unprotected data region can be determined. Accordingly, when a tag name in the unprotection list does not coincide with a tag name that is contained in the unprotected data region, the data in the unprotected data region is determined to be abnormal. Thus detection of the tampering of unprotected data and sender authentication can be performed.

Further, data which requires a substantial amount of time for encryption and decryption can be placed in the unprotected data region. This eliminates the necessity of encryption and decryption of such data. Accordingly, the amount of time that is necessary for encryption and decryption can be greatly reduced as compared with the case where the entire transmission data is encrypted and the entire reception data decrypted. Further, reliability of the data that is placed in the unprotected data region is maintained through the unprotected data validation.

In addition, data that has been placed in the protected data region, and data placed in the unprotected data region, which have been through a signature validation and unprotected data validation, and then determined to be validated as a result, are thus unlikely to be tampered with. Accordingly, an application section, which receives data having been through such validation, is not required to confirm a region from which the data has been sent. As a result, the processing speed of the application section increases.

The Examiner asserted that section 2.3 of Eastlake discusses "core validation," "reference validation" and "signature validation," thereby describing that information from an authentication information region is used for validating the unprotection list, and information from the unprotection list is used for validating the unprotected data. Again, however, the Examiner's assertion is respectfully submitted to be unreasonable.

Section 2.3 merely describes core validation, which is a combination of the reference validation, validation based on a comparison of digest values, and the signature validation, which is validation using a code. In other words, section 2.3 is merely describing a general digital signature system that is based on an authentication technique using hash values and an authentication technique using a public key cryptosystem. Section 2.3 neither discloses nor suggests providing, in the protected data region, and unprotection list including a list of tag names.

In reference validation as discussed in Eastlake, it is determined, based on a comparison of digest values, whether data is tampered with. In signature validation, sender authentication is performed using the public key cryptosystem.

The protected data authentication unit of, for example, claim 46, determines, based on a comparison of digest values, whether data has been tampered with, and also performs sender authentication by using the public key cryptosystem. The unprotected data authentication unit as also for example recited in claim 46 determines the validity of each piece of data in the unprotected data region by using the tag name list (unprotection list) from the data validated by protected data authentication unit.

Accordingly, it is respectfully submitted to be clear that the present claims are not directed to the so-called core validation, including reference validation and signature validation, of Eastlake. Indication of such is respectfully requested.

Further, indication of the allowability of all of the independent claims at this point in time is requested. Should the Examiner believe that the rejection should be maintained, the Examiner is respectfully requested to address, with specificity, the above raised points, and describe, with specificity, how Eastlake in fact discloses each of the elements of the claim, including an unprotection list in a protected data region of tag names indicating types of data included in an unprotected data region, and the determination of whether data included in the unprotected data region is valid by coincidence of the tag names of the data in the unprotected data region with the tag names from the unprotection list.

In view of the above remarks, it is submitted that the present application is now in condition for allowance, and the Examiner is requested to pass the case to issue. If the Examiner should have any comments or suggestions to help speed the prosecution of this application, the Examiner is requested to contact Applicants' undersigned representative.

Respectfully submitted,

Takuya KOBAYASHI et al.

By:__________________
Nils E. Pedersen
Registration No. 33,145
Attorney for Applicants

NEP/krg
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
April 23, 2007